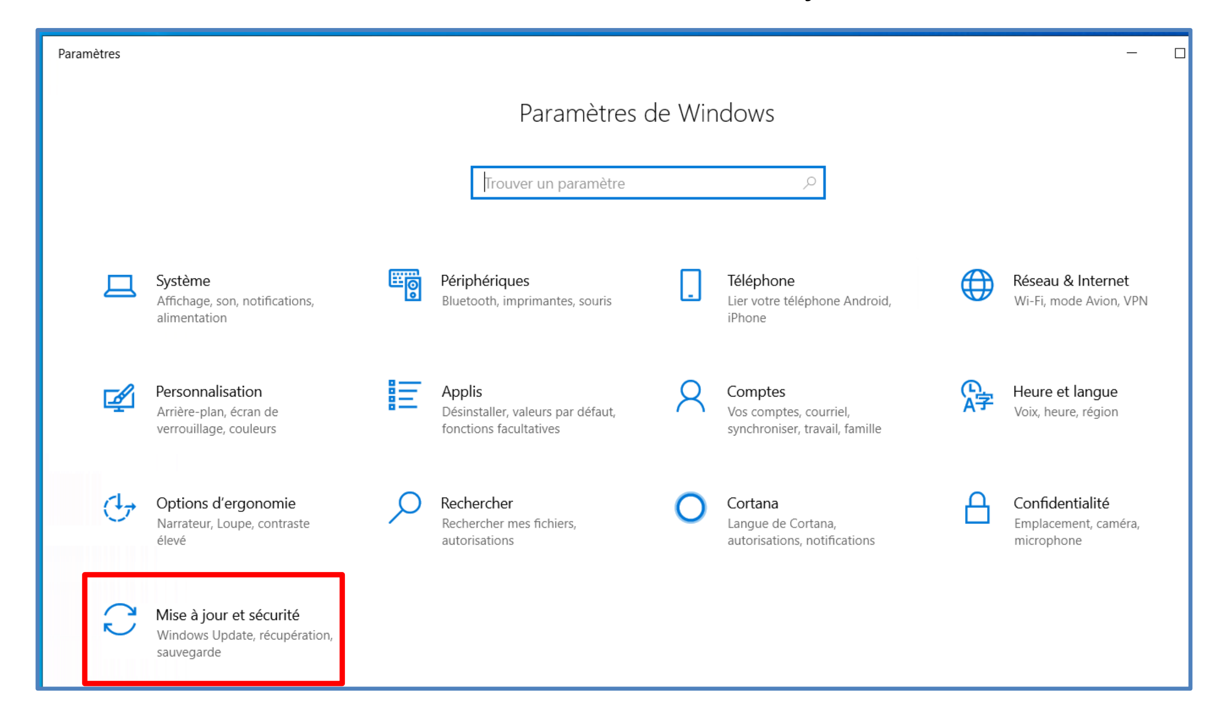
Exercice 1 – Malware - Cheval de Troie (Trojan)

IMPORTANT: Créez un nouveau document Word et enregistrez-le comme VotreNom_Lab6.docx. Il y aura trois captures d'écran que vous devez coller dans ce document.

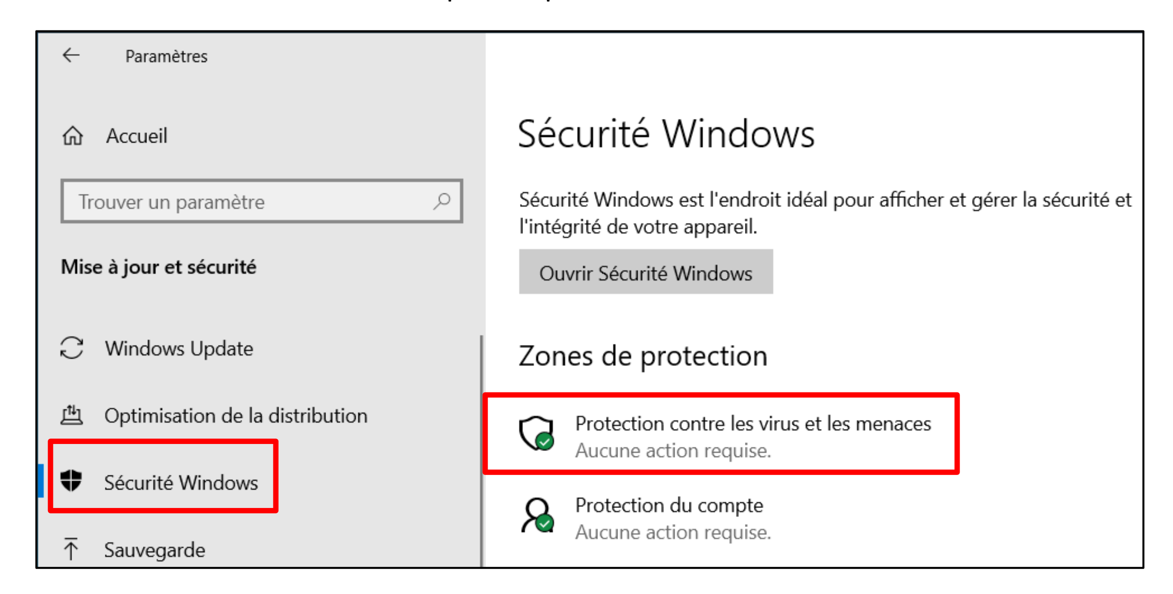
Étape 1 – Désactiver les antivirus (pour être capable d'installer un Malware) :

Pour tester un Malware, vous devez avant désactiver les antivirus installés sur l'ordinateur.

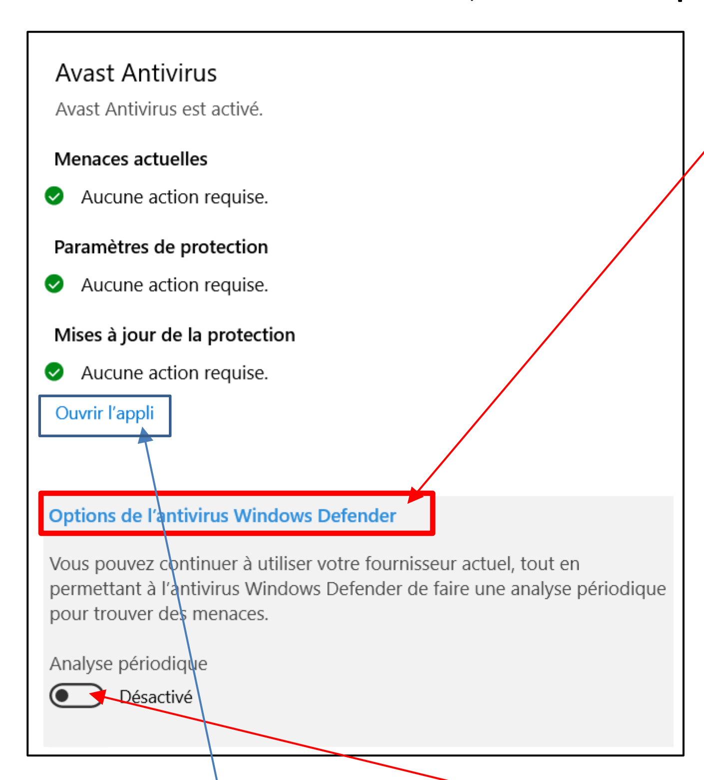
1. Ouvrez les **Paramètres** de Windows et sélectionnez **Mise à jour et sécurité.**



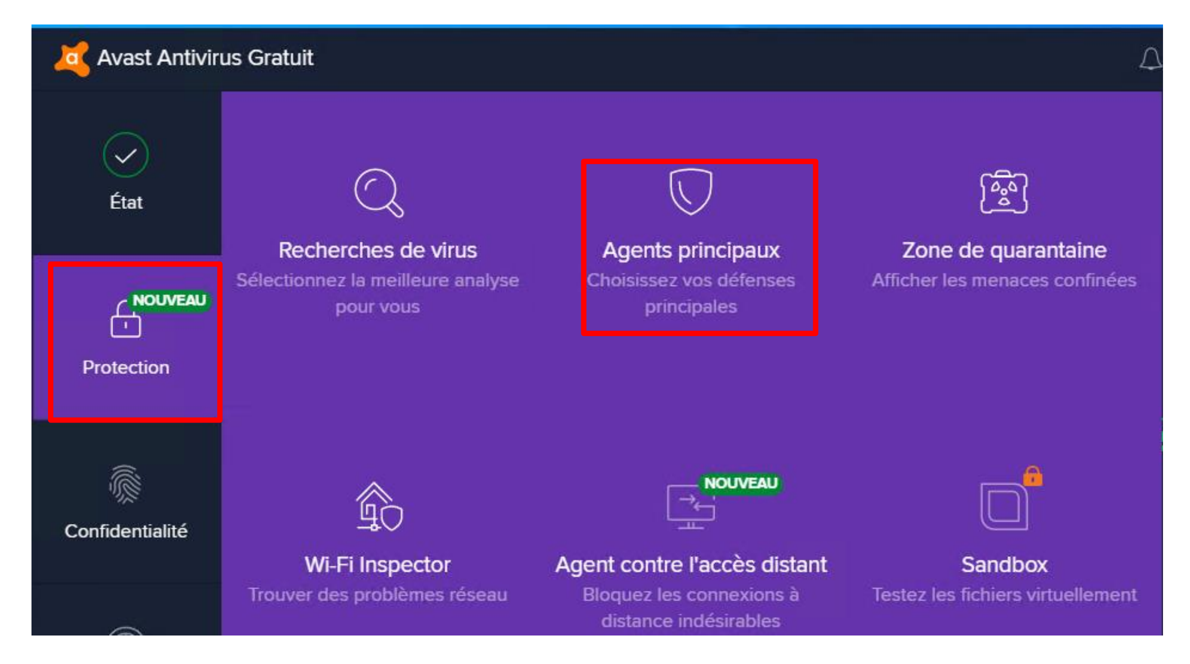
2. Sélectionnez **Sécurité Windows** puis cliquez sur **Protection contre les virus et les menaces**



3. Dans la fenêtre **Sécurité Windows**, sélectionnez **Options de l'antivirus Windows defender**



4. Vous trouverez que **Windows defender** est déjà désactivé par défaut, car c'est **Avast Antivirus** qui protège l'ordinateur maintenant.
5. Cliquez sur **Ouvrir l'appli**, pour ouvrir **Avast Antivirus**.
6. Sélectionnez **Protection** puis **Agents principaux.**



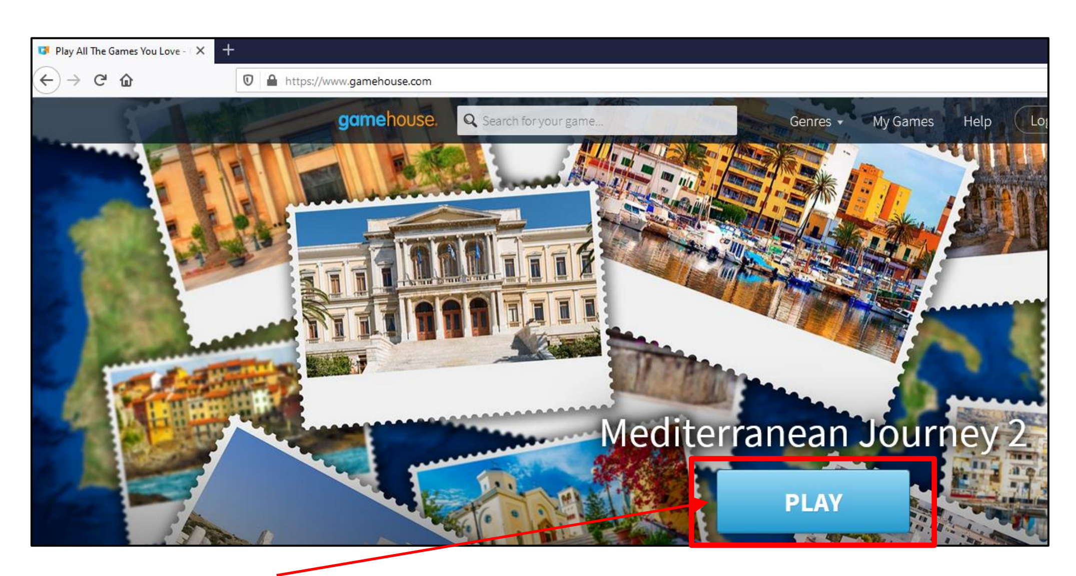
7. Cliquez sur chaque bouton pour la désactiver. Choisissez **Arrêter indéfiniment** puis cliquez sur « **OK, Arrêter »**, pour confirmer.



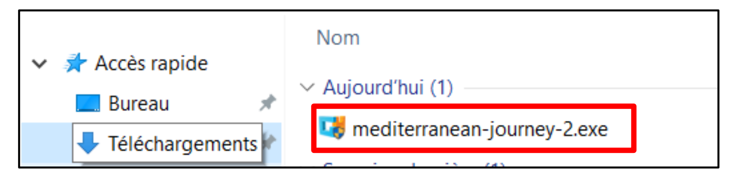
8. Une fois terminé, **fermez toutes les fenêtres ouvertes sur votre Bureau**.

Étape 2 – Installer un Malware :

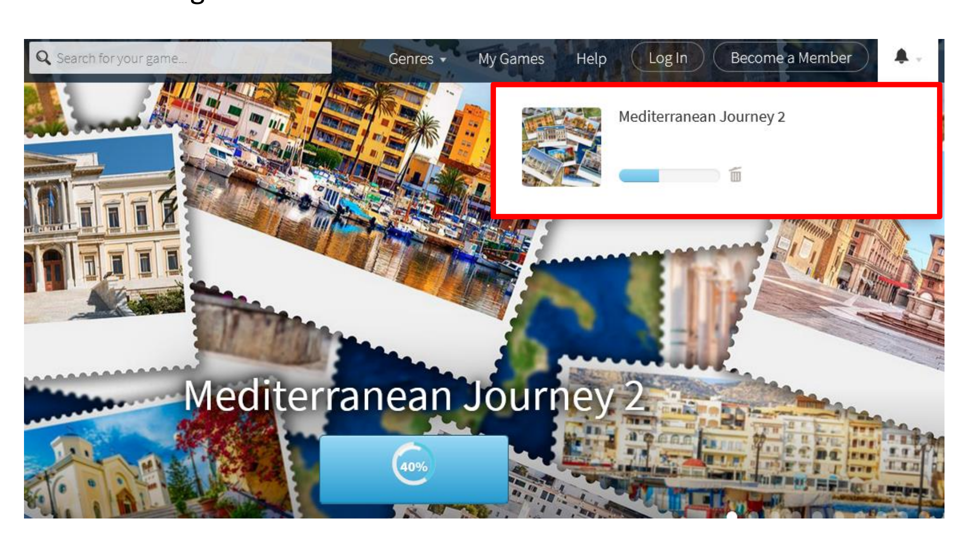
1. Ouvrez **Microsoft Edge** et aller sur le site :
   https ://www.gamehouse.com/games/mediterranean-journey-2



2. Cliquez sur **PLAY**, au-dessous de **Mediterranean Journey 2.**
3. Le fichier **mediterranean-journey-2.exe** sera téléchargé.
4. Gardez **Microsoft Edge** ouvert, et allez dans le dossier **Téléchargement** pour installer le fichier téléchargé.



5. Attendez que le fichier s'installe. Vous pouvez voir **l'état de l'installation** dans la page ouverte de Microsoft Edge.

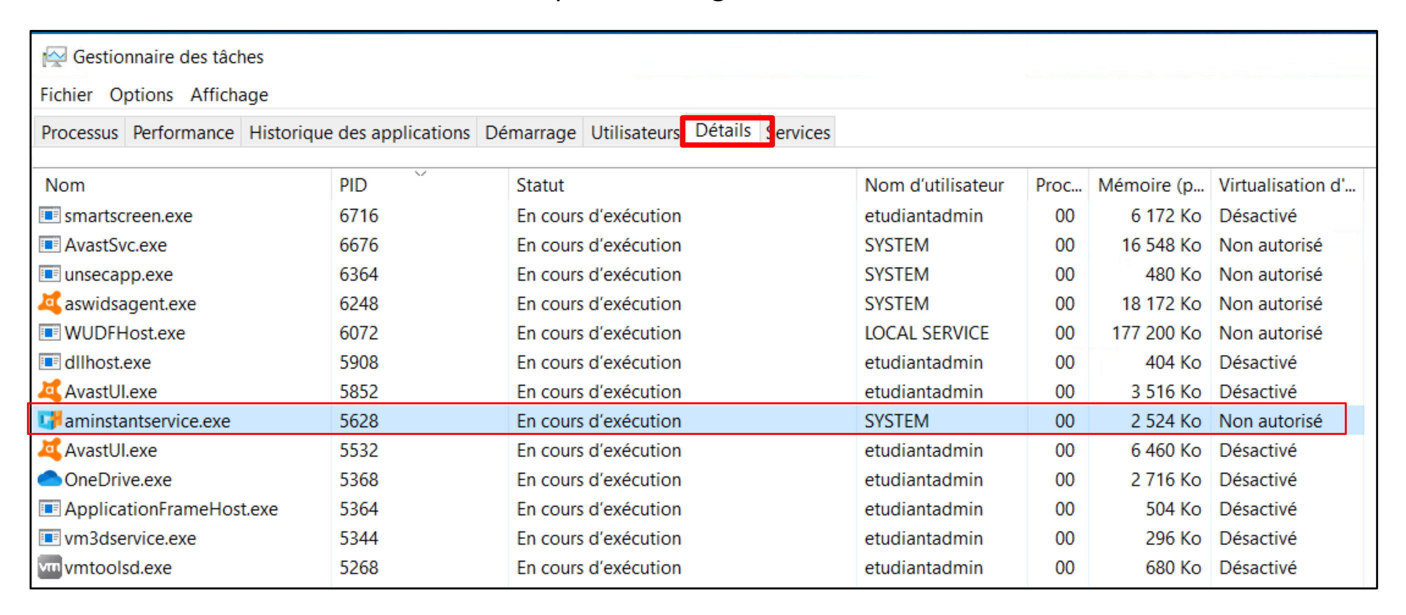


6. Une fois installé, **fermez Microsoft Edge.**

7. Même après avoir fermez Microsoft Edge, un **Malware caché appelé « aminstantservice.exe » est installé sur votre ordinateur!!**

8. La seule façon de le voir c'est avec le **Gestionnaire des tâches.**

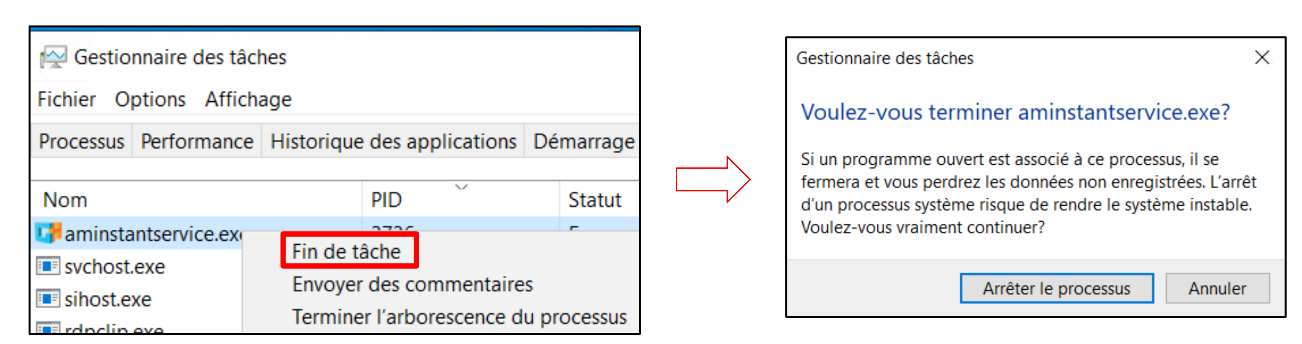
9. Ouvrez le **Gestionnaire des tâches** et cliquez sur l'onglet **Details.**



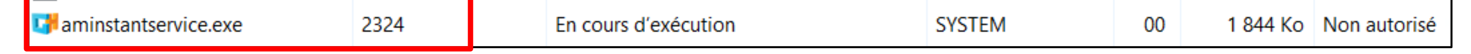
10. Vous allez trouver le processus **« aminstantservice.exe »** caché dans la mémoire comme un processus.

IMPORTANT 1 : Prenez une capture d'écran du Gestionnaire des tâches et mettez-la dans le doc Word.

11. Cliquez avec le bouton droit de la souris sur **aminstantservice.exe**, sélectionnez **Fin de tâche** pour arrêter ce processus. Cliquez sur **Arrêter le processus.**



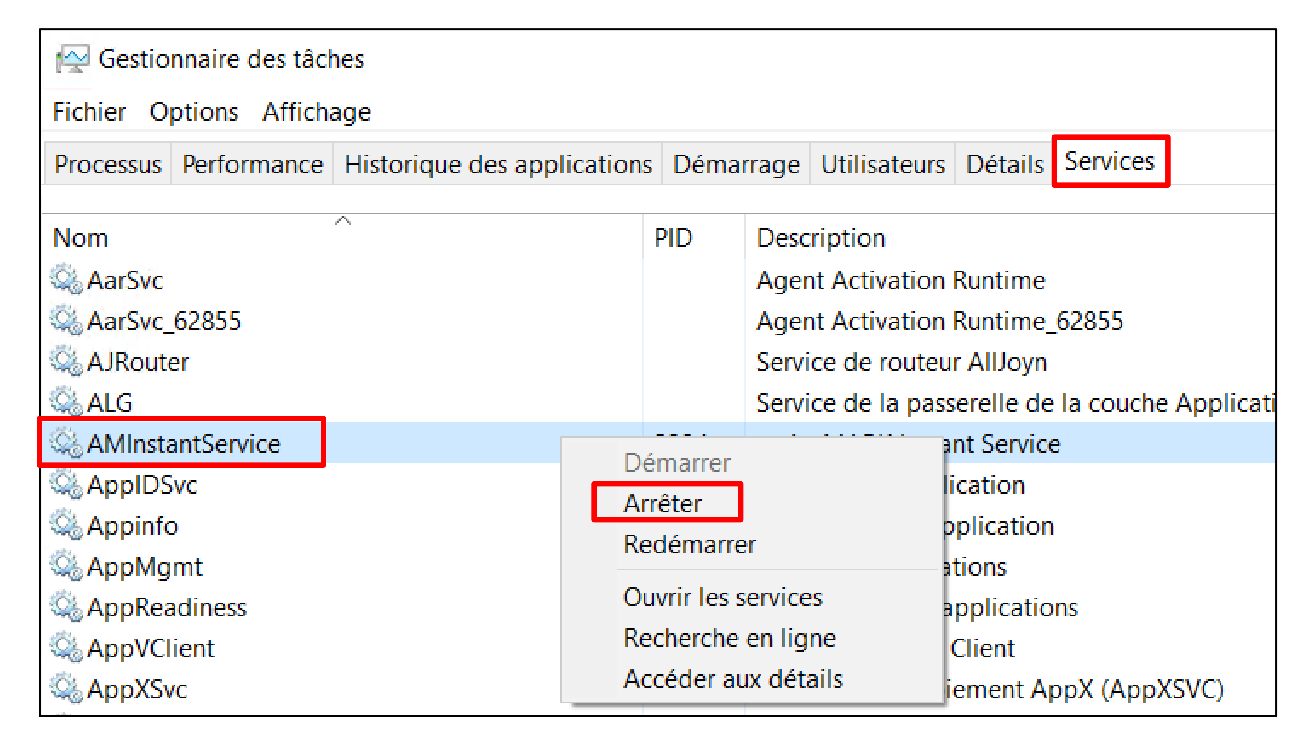
12. Attendez quelques secondes. Vérifiez encore une fois la liste des processus sous l'onglet **Détails**, vous trouverez que le processus **aminstantservice.exe** retourne encore une fois sous l'onglet **Détails!!**



Étape 3 – Arrêter le Malware :

Comment alors arrêter et supprimer ce Malware?

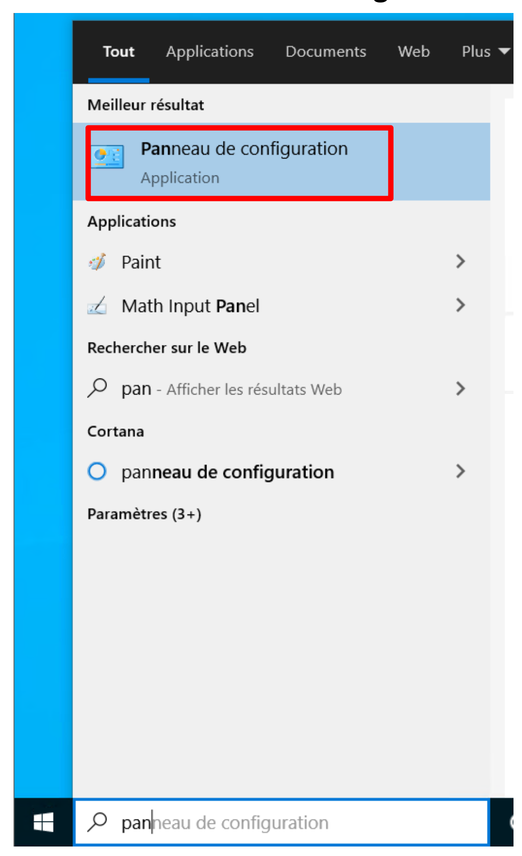
1. L'application de ce malware est installée comme **un service réseau**. La seule façon de terminer ce processus est d'aller chercher le service associé à ce malware et l'arrêter, pour être capable de le désinstaller par après.
2. Dans le **Gestionnaire des tâches**, cliquez sur l'onglet **Services**. Essayez de trouver le service associé à ce malware : **AMInstantService**.
3. Cliquez avec le bouton droit de la souris sur ce service et sélectionnez **Arrêter.**



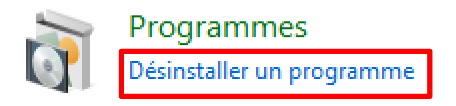
4. Une fois arrêté, retournez à l'onglet **Détails** pour s'assurer que le processus **« aminstantservice.exe »** n'est pas là et qu'il est bien terminé.
5. Fermez le **Gestionnaire des tâches.**

Étape 4 – Supprimer le Malware :

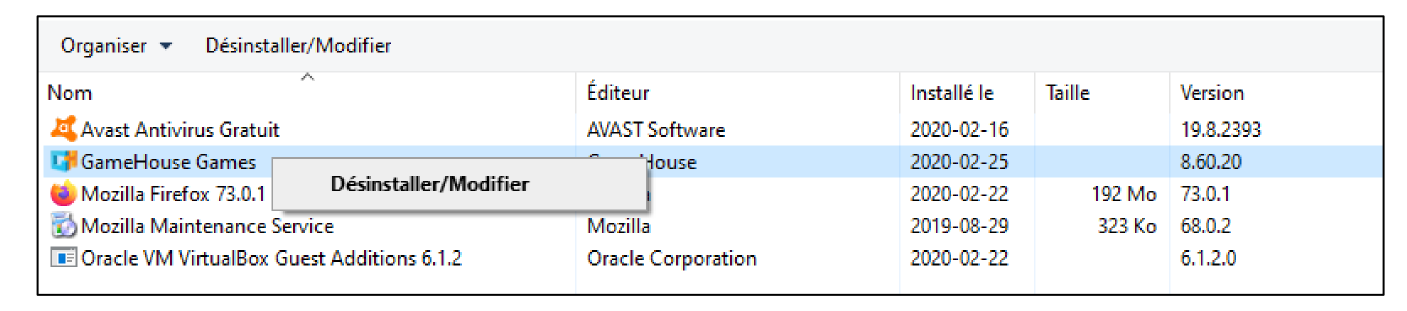
1. Ouvrez le **Panneau de configuration**



2. Cliquez sur **Désinstaller un programme** au-dessous de **Programmes.**



3. Cliquez avec le bouton droit de la souris sur **GameHouse Games** et sélectionnez **Désinstallez/Modifier**.



4. Cliquez sur **Oui** puis **Ok** pour confirmer.

5. Une fois désinstallée, fermez le **Panneau de configuration**.

Exercice 2 – Malware – Keylogger

Étape 1 – Installer un Keylogger :

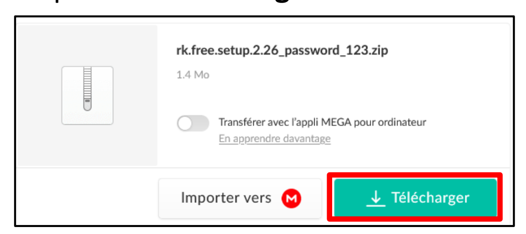
1. Ouvrez **Microsoft Edge** et aller sur le site : https://www.logixoft.com/fr-ca/index
2. Cliquez sur **Télécharger Gratuitement.**



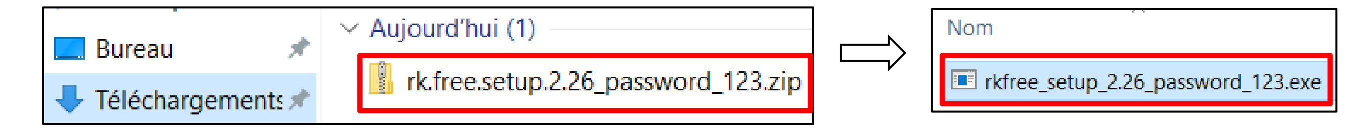
3. Sélectionnez **Télécharger** au-dessous de **BASIQUE.**



4. Cliquez sur **Télécharger.**



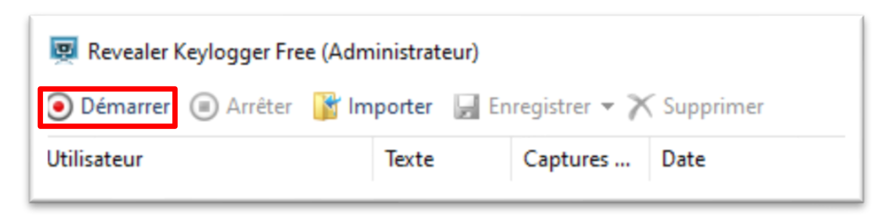
5. Une fois téléchargé, fermez **Microsoft Edge** et allez dans le dossier **Téléchargement.**
6. Double-cliquez sur le fichier **rkfree_setup _2.26_password_123.zip** pour l'ouvrir puis double-cliquez sur **rkfree_setup _2.26_password_123.exe** pour l'installer.



7. Entrez le mot de passe **123**, puis cliquez sur **Installer maintenant.**
8. Une fois installé, gardez la fenêtre **Revealer Keylogger Free (Administrateur)** ouvert et fermez toutes les autres fenêtres.

Étape 2 – Démarrer et cacher le Keylogger :

1. Pour configurer le Keylogger, cliquez sur **Démarrer.**



2. Pour **cacher** le **Keylogger**, fermez la fenêtre de l'application **Revealer Keylogger Free (Administrateur)**.

3. Vous recevez un message qui vous indique que vous devez cliquer sur **CRTL + ALT +F9** pour afficher le **Keylogger.** Cliquez sur **OK.**

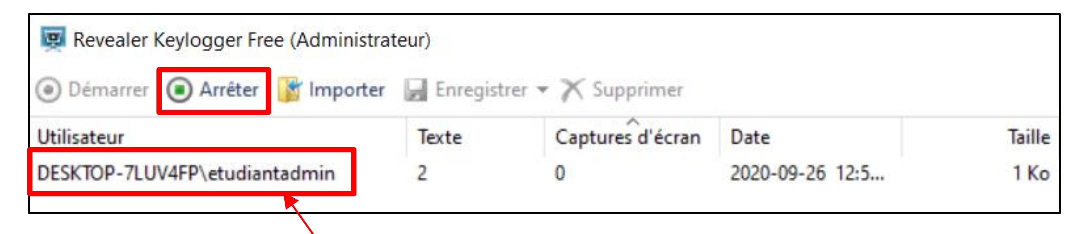


Étape 3 – Tester Keylogger :

1. Pour tester Keylogger, ouvrez **Microsoft Edge.**
2. Allez sur le site du Moodle : https://cmontmorency.moodle.decclic.qc.ca/login/index.php
3. Tapez votre **nom d'usager** et **un mot de passe incorrect.**
4. Fermez **Microsoft Edge.**

   Keylogger a enregistré toutes les frappes de votre clavier, incluant le nom de l'application utilisée.

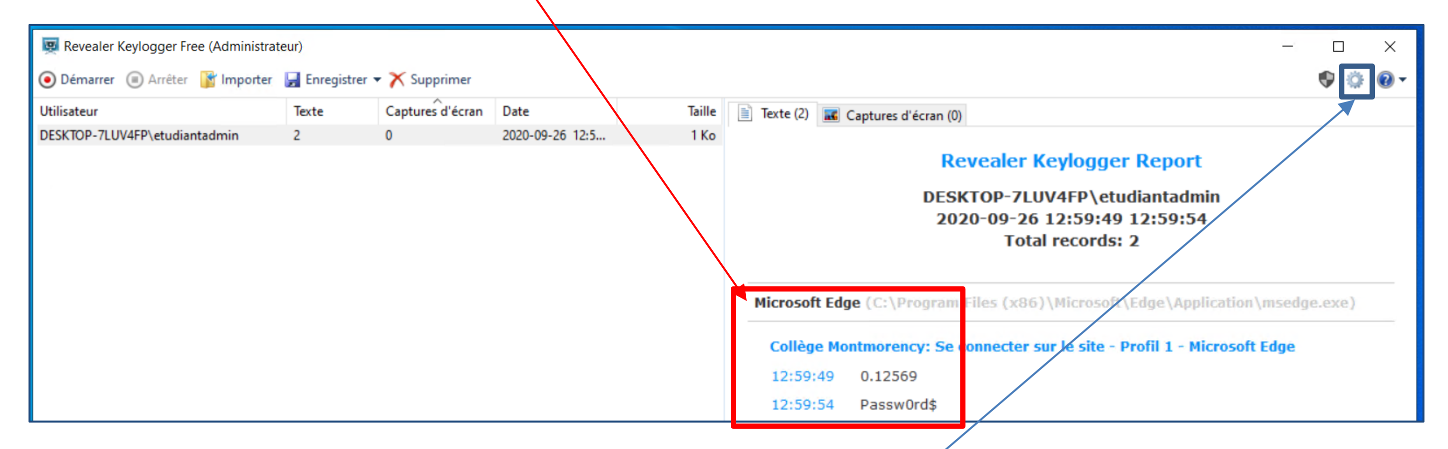
5. Pour ouvrir Keylogger et vérifier s'il a bien capturé les frappes de votre clavier, cliquez sur : **CRTL + ALT +F9**.
6. Dans la fenêtre **Revealer Keylogger Free (Administrateur)**, cliquez sur **Arrêter.**



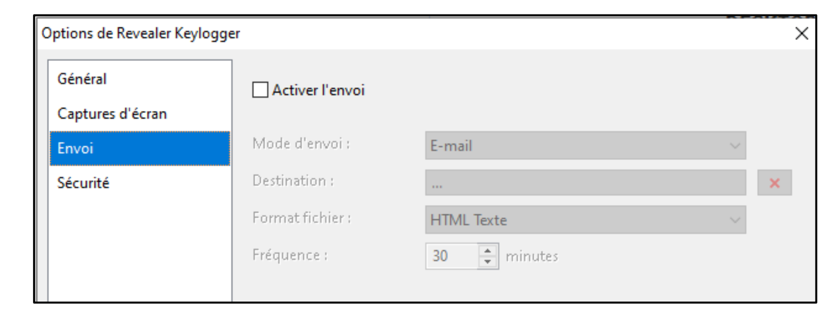
7. Cliquez sur **DESKTOP-7LUV4FP\etudiantadmin**

IMPORTANT 2 : Prenez une capture d'écran de la fenêtre ci-dessous fenêtre et mettez-la dans le doc Word.

8. **Revealer Keylogger** créera un rapport qui contient les frappes de votre clavier (nom d'utilisateur et mot de passe de Moodle)…



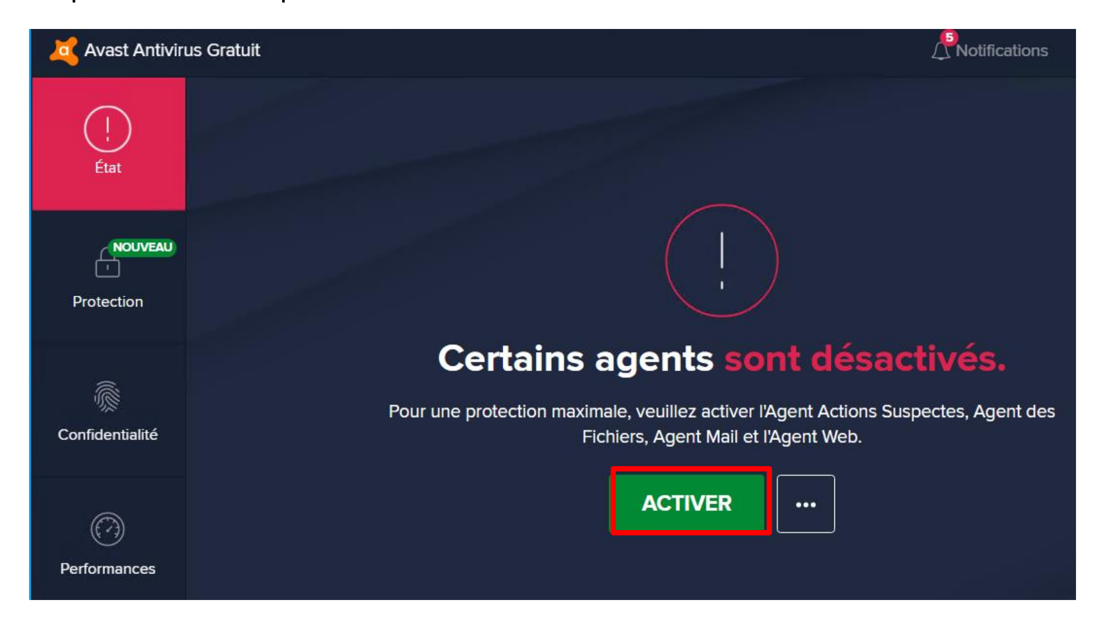
9. Vous pouvez aussi configurer **Keylogger** pour vous envoyer ce rapport par courriel.
10. Cliquez sur **Options**, dans le côté droit haut de la fenêtre.
11. Dans la fenêtre **Options de Revealer Keylogger** vous pouvez configurer ces options. *(Vous devez avoir la version payante pour faire cela).*



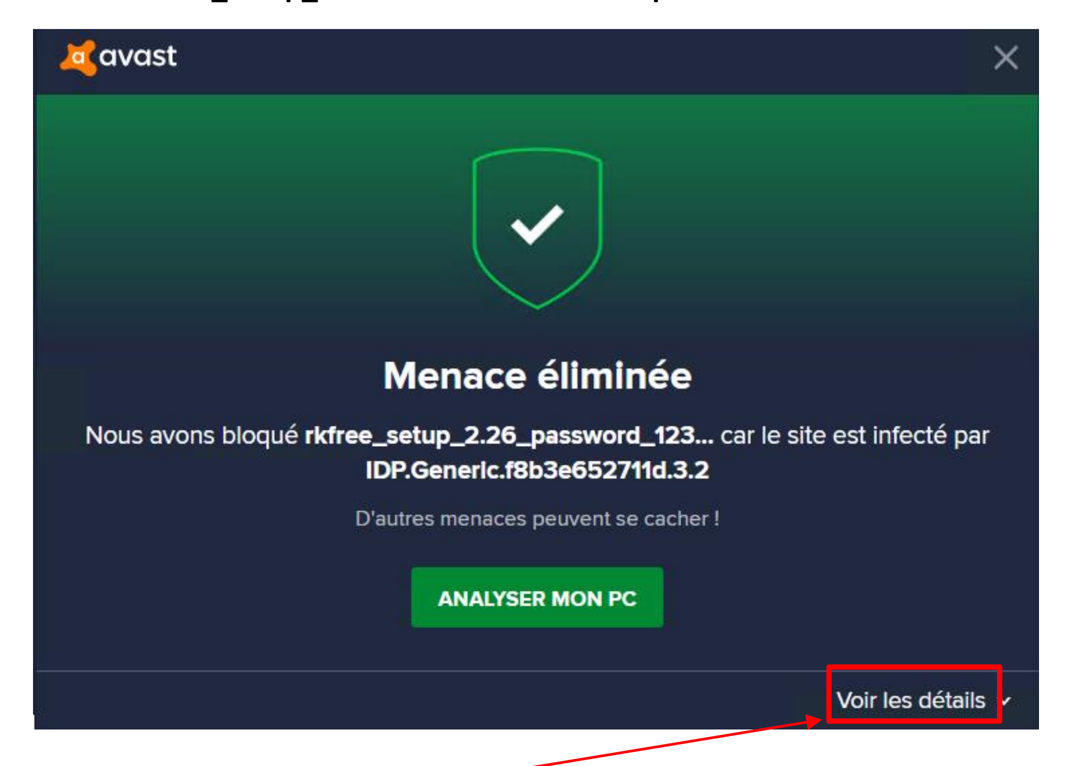
12. Fermez toutes les **fenêtres de l'application Keylogger.**

Étape 4 – Détecter et supprimer le Malware Keylogger

1. Ouvrez **l'antivirus Avast** pour le réactivez**.**
2. Cliquez sur **Activer** pour activer l'anti-virus.



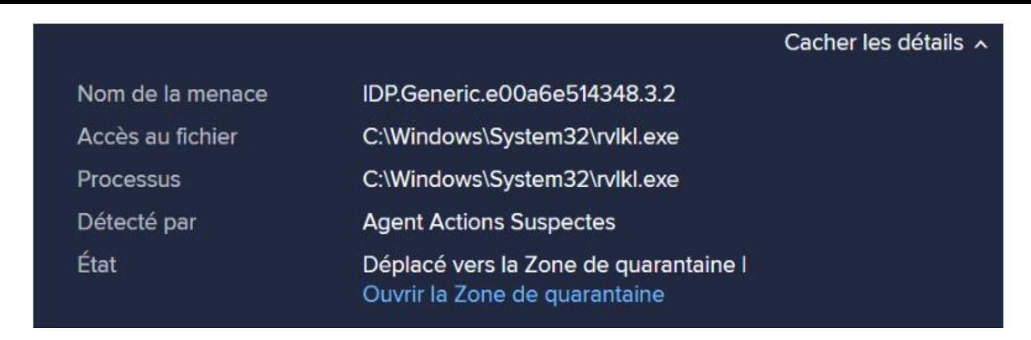
3. Une fois activé, attendez une minute, Avast va scanner votre ordinateur et va détecter le keylogger malware **rvlkl_setup_2.26** et le mettra dans **la quarantaine.**



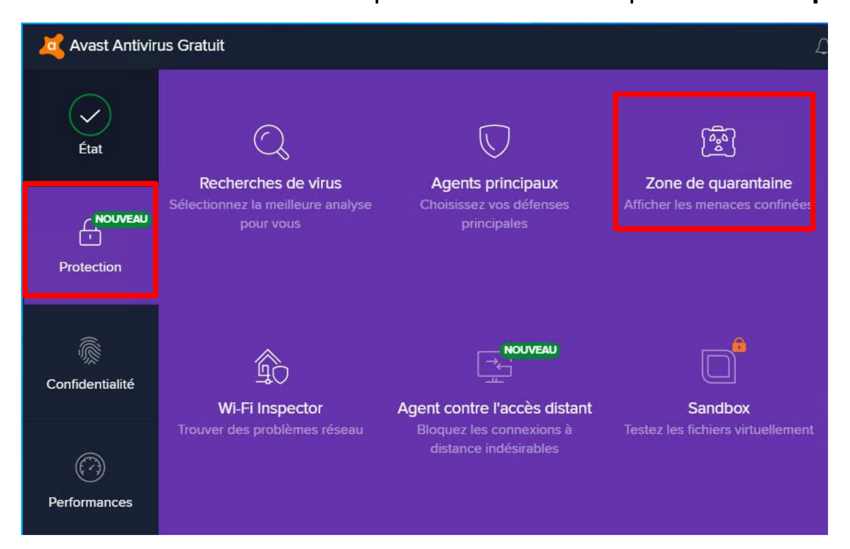
4. Cliquez sur **Voir les détails.**

5. Avast affichera l'emplacement de ce malware sur votre disque **C:**

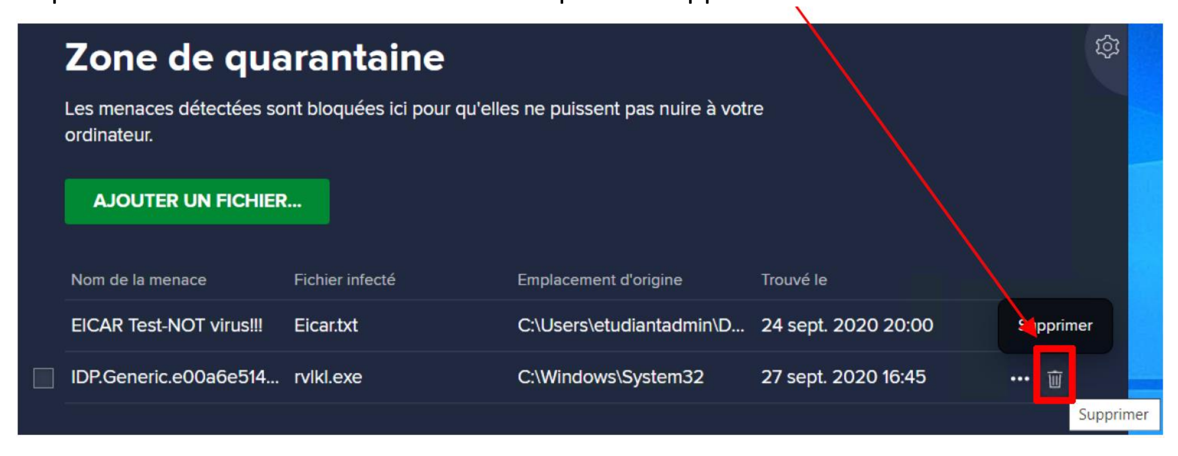
IMPORTANT 3 : Prenez une capture d'écran de cette fenêtre ci-dessous et mettez-la dans le doc Word.



6. Fermez cette fenêtre et cliquez sur **Protection** puis **Zone de quarantaine.**



7. Cliquez sur la corbeille à côté du Malware pour le supprimer.



8. Fermez la fenêtre de l'Anti-virus Avast

9. Cliquez sur **CRTL + ALT +F9**, vous allez voir que le malware **Keylogger** ne s'ouvre pas car il était éliminé par AVAST…

10. Déconnectez-vous de Windows et fermez la connexion VPN.